

Article 34 Amendment

P 1, L23 :

“Patent Kokai 2001” → “Patent Kokai 2002”

P 3, L22:

“(“T” hereafter) ” → “(“T” or “destination terminal” hereafter)”

P 3, L26:

“(“D” hereafter) ” →

“(“D” or “mapping notification system” hereafter)”

P15, L 4:

“when simply gives its identity, can confirm ” →

“when T simply gives its identity, S can confirm ”

P31, L 7:

“T(4100)” → “S”

P65, L 4:

“enables to detect” → “enables S to detect”

P73, L11:

“convergence 4” → “convergence 3”

CLAIMS:

27.12.2004 受理

手 続 補 正 書
(法第 11 条の規定による補正)

特許庁長官

殿

1. 国際出願の表示

PCT/JPO3/16538

2. 出願人

氏 名

福島 一

FUKUSHIMA, Hajime

あて名

〒165-0027 日本国東京都中野区野方二丁目62番3号

2-62-3, Nogata

Nakano-ku, Tokyo 165-0027

国 籍

日本 JAPAN

住 所

日本 JAPAN

3. 補正の対象

明細書、請求の範囲

4. 補正の内容

明細書の内、誤記を訂正したものと差替える。

明細書の内、翻訳のための主語を追加したものと差替える。

明細書1頁17行目 特開2001 -> 特開2002

(文献番号のタイプミスを訂正)

明細書3頁26行目 「T」とする -> 「T」亦是「あて
先端末」ともいう(同じ物を指す用語の紛らわしさに対応)

明細書3頁30行目 「D」とする -> 「D」亦是「マッ
ピング公示システム」ともいう(同前)

明細書17頁29行目 単に名乗るだけで到達性確認はできる

一> 単に T が名乗るだけで S は到達性確認をすることができる（翻訳の為に主語を補った）

明細書 36 頁 22 行目 T (4100) 一> S (誤記の訂正。T が T をというのは、誤りである)

明細書 59 頁 13 行目 のの 一> の (誤記の訂正)

明細書 75 頁 20 行目 場合をも、検知できる 一> 場合をも、S は検知できる（翻訳の為に主語を補った）

明細書 78 頁 4 行目 をから 一> から (誤記の訂正)

明細書 84 頁 4 行目 収束 4 一> 収束 3 (誤記の訂正)

請求の範囲 第 1 項～第 51 項を補正し、第 52 項を追加する。

6. 添付書類の目録

明細書 (1 頁、3 頁、3/1 頁、17 頁、36 頁、59 頁、75 頁、78 頁、
84 頁) 各一通

請求の範囲 (86 頁乃至は 94 頁、94/1 頁) 各一通

(発明の名称)

- 静的な識別子と動的な住所が関連付けられることによってホスト到達性が得られる網にあって、到達性を確認するための通信モデル、信号、方法および装置

(技術分野)

- 本発明は、蓄積交換型の通信網において、あて先端末を発見する過程における不備を解決する通信モデル、信号、方法および装置に関する。
- 詳しくは、静的な識別子を動的な住所に変形することによって、あて先端末への到達性を発信元を提供する場合において、発信元があて先端末への誤った到達性を持つ場合と正しい到達性を持つ場合とを峻別する。

(背景技術)

- (特許文献1) 特許公表 2001-519607 亦はWO 99/18515 (米インテル) 静的な識別子を動的に割当てられたネットワーク・アドレスに変形する方法および装置
- (特許文献2) 特開 2002-135301 (NTT) IPアドレス情報通知方法およびIPアドレス情報通知装置並びにこのプログラムを記憶した記憶媒体
- (特許文献3) 特開 2002-318737 (インデックス) 管理サーバ
- (特許文献4) 特開 2002-281032 (東芝) 監視対象切替プログラム、方法及び監視システム
- (特許文献5) 特開 H7-200502 (オムロン) トランザクション処理システムに関する二重化装置

- インターネット(=the Internet)は非常に多数の計算機と計算機による網(以下、単に「網」とする)から構成され、これらはTCP/IPプロトコルを用いた通信リンクを通して世界的な規模で相互に接続されている。相互に接続された計算機は、電子メール、ゴーファー、およびワールドワイドウェブ等の、様々なインターネットサービスを利用して情報をやりとりしている。

- インターネットは、網割当て団体から一意に割当てられたIPアドレスによって、そのホストを識別している。IPアドレスは、計算機が処理し易いように固定長の数字の羅列として表現されており、人間にとっては無意味綴りであり、覚えたり毎回間違えずに入力したりするのが困難である。TCP/IP網においては、ホストを特定する為には少なくともIPアドレスが必要であり、IPアドレスでホストを特定

かける行為を伴うものをいうが、近年ケーブルテレビやデジタル加入者回線、光ファイバや衛星リンク等をアクセス回線に用いた定額制のIP接続業務等によるアクセス回線の多様化により、必ずしも電話をかける行為を必要としなくなっている。これら近年の常時接続型と呼ばれるインターネット接続業務は、単に接続時間による課金体系でなくなったことを意味し、ルータのセッション異常終了(停電

- 5 等)、回線の異常、センタの故障やメンテナンス等により接続が異常切断された場合や接続業者もしくはダイヤルアップするホストの無通信タイマによって回線が切断された場合等に再接続すると、IPアドレスが変わる場合があるという点で専用線による接続と異なる。また、移動体通信端末の場合において、無線基地局を移動した場合等にIPアドレスが付け変わることがある。このような場合(すなわちハンドオーバーした場合)にも、本明細書では便宜上、端末ノードのIPアドレスが変化するという点で、
- 10 ダイヤルアップに含めることとする。

- そこで本発明では、従来の専用線による接続に代表される網割当団体から恒常的な網の割当てを受けて接続する場合かプロバイダ(あるいはIPアドレスの割当てを受けた各利用組織)から恒常的なIPアドレスの割当てを受けて接続する場合と対比して、プロバイダ(あるいはIPアドレスの割当てを受けた各利用組織)からの一時的な利用を前提としたIPアドレスの割当てを受けて接続することを
- 15 (モデムを用いて電話をかけるという行為を伴わず、DHCPやPPPoE等による割当てであったとしても)「ダイヤルアップ接続」といい、一時的なIPアドレスの割当てを受けるための動作をすることを「ダイヤルアップする」という。また、IPアドレスの一時的な割当てそのものを「ダイヤルアップ」ということとする。

20 ダイナミックDNS特有の問題

- 従来の技術では、IPアドレスが変化するホストでのインターネットサービスの提供はできなかったが、ごく最近になってダイナミックDNSを用いることによって、限定的に(グローバルサービスとしてのDNSは固定IPアドレスが必要なことからDNSを除く)インターネットサービスを提供できるようになった。しかし、ダイナミックDNSを用いることに特有の以下の問題点があった。これを以下、図01乃至図12
- 25 にダイナミックDNS特有の問題の発生から収束までの過程を紙芝居形式で説明する。

図01。管理対象機器(以下、「T」亦は「あて先端末」ともいう)(4100)からプロバイダ(以下、「P」とする)(4000)へダイヤルアップ(PPPoE等を含む)する。

図02。T(4100)はP(4000)からIPアドレスの動的割当てを受ける。この時、割当てを受けたIPアドレスを仮に172.16.100.100とする。

- 30 図03。T(4100)はダイナミックDNSサーバ(以下、「D」亦は「マッピング公示システム」ともいう)

(1000)へDNSの更新要求をし、こ

1、前記同様、ウェブページの例のように、もちろん人間が見ればわかる。いわゆる人間による目視確認である。

仮に見てわからなくても、調べればわかる。このとき、大体次のようなことを調べる。

2、nslookupでもわかる。pingでもわかる。

5 3、ホストそのものが名乗るので、わかる。ただし、ここでホストが名乗るとは、サービスと呼ばれる通信プログラム(以下、この通信プログラムを「Daemon」と呼ぶこととする)を経由して、名乗ることとする。また、従来は、ここで名乗った返事を聞いた通信の相手方が、それに基づいて特別なアクションを起こすことはなかった。ここで特別なアクションとは、例えばそれによって接続の許可拒否を判断する等である。

10 4、アカウントがあれば、パスワード認証を利用することもできる。

さて、本発明の前提であるT(4100)がダイヤルアップのホストである場合に戻るとしよう。

1については、到達性確認の目的は人間だけでなく機械にもわかるようにすることなので、ここでは考慮しない。

2のnslookupは、既に説明した通り、本当に正しい相手先かどうか不明なままである。pingも同

15 じである。

4は、サーバにおけるアカウントの問題である。本発明は相手先サーバ(あるいはホスト)にアカウントがあることを前提としていない。そのため、アカウントがあることを前提としての認証については、別論である。

さて、では3はどうであろうか?

20

Daemonは通信ポートを開けて接続を待つ常駐型のプロセスのことであるが、だいたいホスト名、プログラム名、バージョン名等を名乗るものである。

よって、3は使することができる。

これは、T(4100)が固定IPアドレスの場合には、当然に通信の開始時点において、行なっていたことである(ただしこれを元に通信をするかしないかを判断することは、従来はされていない)。

25 ここでホスト名に対するアクセスに対して、Daemonが名乗るということは、単に自己の識別情報を示しているに過ぎない。

これは認証という概念には含まれないものである。

そして、単にTが名乗るだけでSは到達性確認をすることができる。

30

別名(=CNAME) → ホスト名 → IPアドレス

電話番号 → ホスト名 → URI → IPアドレス

答えるべき返事は、上記のうち、

IPアドレスを除く、

- 5 DNS への最初入力である静的な識別子の、あるいはDNS での識別子変形過程上で得られる(中間過程の)識別子の、
いずれであってもよい。

なお、上記のうち、別名で始まるものは、特別な意味を持つ場合がある。

- 10 第一に、別名によって、別のDNS 上のホストを参照させることは従来知らされてきたことである。すなわち、再帰性ENUM以前からあった。

第二に、その別のDNS 上でポイントされたT(4100)が動的更新される場合である。文字列変形を無視して単に動作として考えたとき、ENUMと同じ動作といえることができる。

ここでカウンターサインを複数返してもよいものとする、エンド・エンドの場合のみならず、名前検

- 15 索過程における中間過程のホスト(この場合はDNS)に対しても、到達性を確認することができる。Sでは複数返された答えるべき返事の中から、目的たる答えるべき返事を抽出すればよい。

この際、1のカウンターサインの中で、複数の答えるべき返事を返す方法と、カウンターサインによってキャリアされる答えるべき返事は1のみに固定し、複数のカウンターサインを返す方法とがある。

このように、複数のカウンターサインを返すことは、概ね2つのことに貢献する。

- 20 1つは、単一のT(4100)において、複数の識別を可能とすること。
もう1つは、名前変形過程上の中間段階におけるノードがカウンターサインを複数返すことによって、追跡性を増すことが可能となること。この際、Sでは、中間ノードがした応答の中から、お目当てのT(4100)を示す答えられるべき返事を抽出するようにすればよい。こうすることによってtracerouteのように、中間ノードの到達性を確認することができ、障害時の障害個所の特定に多に役立てることができる。
- 25

設計思想

網管理とは

- ここで念の為に網管理の必要性について説明する。まず、用語の説明として、網管理自体は、いわゆる構成管理や課金管理等をも含む通常の管理の概念であって、その対象を網としているものであ
- 30

(2000)やD(1000)が外部の網に属しているという点で、表03の②④⑥の場合に相当する。

なお、TCP/IP以外のプロトコルはルーティングされないものとする。

- P(4000)はT(4100)を含む網であると考えられるので、今度はP(4000)の観点から、機能が複合した場合の特徴について説明する。なお、図38ではT(4100)を含む網1がP(4000)にあたる。P(4000)がDHCPである場合であっても、網1はDHCPサーバを含む網であるとして、以下説明する。また、網2はここでは単に網1でない網とする。

機能が複合した場合の特徴

- 10 S-1(2000)とP(4000)が一体となっている場合。図38のパターン1の場合である。

P(4000)の網に属するT(4100)に関して、後述する条件1によって、S-1(2000)は本発明によらずにT(4100)の到達性を確認出来る。しかし、T(4100)とD(1000)は異なる網に属しているため、実像と写像の関係の正しさについて、S-1(2000)は確認することができない。すなわち、T(4100)に関してD(1000)によって獲得するホスト識別性については、本発明の到達性確認を要する。

15

S-1(2000)とD(1000)が一体となっている場合。図38のパターン2の場合である。

アドレス確認は不要である。この他別の効果もあるが、これについては後述する実際的应用の第三のフィルタ例で説明する。

- 20 D(1000)とP(4000)が一体となっている場合。図38のパターン3の場合である。

IPアドレスの割当て主体であるところの、T(4100)を含む網すなわちP(4000)と、D(1000)とが同一の組織に属する場合である。

先に説明したように、一般的にこの場合は問題がない。

しかし、条件1から、P(4000)がD(1000)を更新する場合は、境界線上の場合である。

- 25 条件1

P(4000)は特別な立場にある。

P(4000)とは、ここではT(4100)に対してIPアドレスを割当てるものをいう。

よって、当然にP(4000)はT(4100)のIPアドレスを把握しているものとする。

そして、当然にP(4000)はT(4100)が接続しているか接続していないかを把握できる。

- 30 以上を条件1とする。

用の端末でなければ、T(4100)が網上に存在しなくなったことを検知することができないことだった。D(1000)はT(4100)を、D(1000)とT(4100)との関係の上でのみ成立つ個体識別という考え方によって識別していたために、T(4100)が専用の端末であることをD(1000)は必須とした。

- 5 しかし、この問題も本発明によって解決された。すなわち、本発明によって、専用の端末である必要がなくなったのである。

ダイナミックDNS特有の問題点のまとめ1で指摘した問題点は、実は事象的な問題点であった。すなわち、目に見える問題点である。そしてこれを解決するためには、特許文献1や特許文献2によるアプローチがあった。すなわち、D(1000)の公示が正しくないがゆえに、D(1000)の公示を是正し

- 10 ようとするものである。しかし、上記問題点は事象であって、原因は他にある。発明者の洞察に拠れば、その原因は実像と写像の不一致である。従来はSの視点がなかったのだ。この視点によって、SがT(4100)への到達性を確認することを実現した。この際Sは、TD間の直接的な関係性に依存することなく、T(4100)とD(1000)からそれぞれ別個に網の構成要件としての4つの要素を得て、その対応の正しさすなわち実像と写像の一致によって、到達性の正しさを確認する。

- 15 この考え方に至った時点で、特許文献1や特許文献2のようなD(1000)がT(4100)を個体識別するという考え方はなくなっている。そしてこの時点で、到達性確認することのできる通信ノードは、Sである以上あらゆる通信ノードである。それゆえ、本発明によって、専用の端末である必要がなくなったのである。

- 20 それでももちろん、到達性確認は、特許文献1や特許文献2が検知することを目指したT(4100)が網
上から存在しなくなっている場合をも、Sは検知できるものである。それゆえ当然に、D(1000)においても到達性確認をすることはできる。そして、既に挙げたような優位性を有する以上、到達性確認は特許文献1や特許文献2に比して、進歩性を否定されるものではない。本発明は、通信における発信元とあて先がエンド・エンドで到達性確認できるようにしたことの特徴を有する。すなわち、本発明の根幹は到達性確認を実現する理論と実装である。ここでは静的な識別子と動的な住所が関連付けられることによってホスト到達性が得られる網にあつては、実像と写像を比較することによって、そのホ
25 スト到達性を確認することができるとの、新たな理論を提示した。

この際、カウンターサインという新規のキャリア信号を提案することによって、前記4つの要素のうち、従来では入手することのできなかった要素(すなわち実像におけるB)を入手することを可能にした。

レス確認をすればよい。実施例1に示した2回目のS216のときに、一定時間待つのではなく、すぐにアドレス確認の過程に戻るようにする。この際、切分の実装にはフラグ等を用いよう。

これを実装的に説明すると、図示しないが図23で説明すると以下のようになる。

最初に到達性確認に成功した場合から説明する。

- 5 S214の後で、フラグを立てる。既に立っている場合はそのまま。そして、T(4100)の住所を記憶して終了する。

次回到達性確認したときは、S202の前で、フラグが立っているかどうかを判断して分岐する。フラグが立っていれば、前記憶された住所を、S204におけるT(4100)を示す住所に代入する。そして、S206から始める。フラグが立っていなければ、通常どおりS202から始める。

- 10 次に到達性確認に失敗した場合である。S216の後で、フラグが立っていればフラグを消す。フラグが元から立っていない場合はそのまま。Tの住所が記憶されていれば、これも消す。そして、次回到達性確認のタイミングが回ってくるまで待つのではなく、すぐにS202に戻り、やり直す。ただし、この際2回目以降のS216に該当する場合があるので、一時フラグ等を用いて永久ループを回避するとよい。

- 15 フラグの立て方は、ここでは到達性あり(S214)の場合に立てたが、逆(S216)にしてもよい。この際、当然にS202以前の分岐も逆にする。

後者のキャッシュをS上に展開する方法では、キャッシュの生存時間経過後、再度名前問合せをすることになる。もちろん、この場合であっても、T(4100)が答えるべき返事として不明な応答を返した場合には、アドレス確認を省略している訳だからすぐさまT(4100)は到達しないと判断するべきでな

- 20 く、アドレス確認からやり直すべきである。

どちらも、名前解決に関するホスト間通信の頻度を減らすことができ、かつキャッシュによる誤認を発生させないようにする効果がある。どちらかという、前者の方がお勧めである。この理由は、T(4100)に到達しなくなるまでの間、名前問合せしないのであるから、結果として名前問合せする頻度が前者の方が少ないことによる。また、Sが網接続機器等の比較的資源に余裕がない装置である場合

25 合には、キャッシュを展開させるような変更が負担である場合等があり、その際にもアプリケーション的解決の方が有利である。

アプリケーション的解決はSとして、S-1(2000)、S-2(5300)を許容する。実際的应用に示した第三のフィルタ例D(1000)をSとする場合と似る。D(1000)をSとする場合には、名前問合せを省略したのではなく、名前問合せが内部的に完結するので、実質的にホスト間の通信を省略したのと同じこ

- 30 とになる。D(1000)とは異なり、内部的な名前解決をすることができないS-1(2000)やS-2(5300)

- 図18 キャッシュの生存時間を示す図である。
- 図19 キャッシュの生存時間の収束1(計測プログラム)を示す図である。
- 図20 キャッシュの生存時間の収束2(計測結果1)を示す図である。
- 図21 キャッシュの生存時間の収束3(計測結果2の続き)を示す図である。
- 5 図22 通信モデルを示す図である。
- 図23 課題を解決するための手段を示すフローチャートである。
- 図24 課題を解決するための手段2(S204のオプション処理)を示すフローチャートである。
- 図25 DIGコマンド 正常出力例を示す図である。
- 図26 DIGコマンド エラー出力例(DNS サーバが存在しない場合)を示す図である。
- 10 図27 DIGコマンド エラー出力例(Tが存在しない場合)を示す図である。
- 図28 SNMP正常出力例(Tが正しい到達性の場合)を示す図である。
- 図29 SNMPエラー出力例(ホストが間違いの場合)を示す図である。
- 図30 SNMPエラー出力例(コミュニティ名が間違いの場合)を示す図である。
- 図31 SNMPエラー出力例(オブジェクトIDの指定間違いの場合)を示す図である。
- 15 図32 BINDにおけるバージョン情報の設定の為にする設定ファイルの変更箇所を示す図である。
- 図33 DIGコマンド 正常出力例を示す図である。
- 図34 DIGコマンド エラー出力例(Tが存在しなかった場合)を示す図である。
- 図35 DIGコマンド エラー出力例(別のネームサーバを参照してしまった場合)を示す図である。なお、バージョン情報が設定されていない場合の標準的な出力例(正常)でもある。
- 20 図36 SMTPサーバ(SENDMAIL)に接続した際の最初のメッセージ例を示す図である。
- 図37 Tのカスタマ網における接続形態を示す図である。
- 図38 各ホストと網の位置関係を示す図である。
- 図39 本発明をいわゆるping代替として用いる場合の動作の違いを示す図である。
- 図40 DNS更新スクリプト・サンプルを示す図である。
- 25 図41 クライアント・サーバ・モデルにおける集約効果を示す図である。

(符号の説明)

記号 名称

- 1000 D。マッピング公示システムである。DNSが代表例であるが、DNSのみを指す訳ではなく、
- 30 特許文献2の場合等も含む。DNSと表記された場合には、DNSのみを指す場合と、DNSでないが

1. (補正後) 静的な識別子と動的な住所が関連付けられることによってホスト到達性が得られる蓄積交換網において、

マッピング公示システム(1000)におけるあて先通信ノード(4100)を示す静的な識別子と動的な住所からなる組の写像と、

あて先通信ノード(4100)における静的な識別子と動的な住所からなる組の実像とを比較することによって、

あて先通信ノード(4100)への到達性の真偽を判定することを特徴とする通信モデル。

2. (補正後) 請求項1の通信モデルにおいて、

以下のシーケンスによって、前記通信モデルにおける比較要素を発信元通信ノード(2000 又は 5300)が知る手順が実行されることを特徴とする通信モデル。

(1) 発信元通信ノード(2000 又は 5300)が、あて先通信ノード(4100)の静的な識別子をキーにマッピング公示システム(1000)に対して要求する名前問合せを行い、

(2) マッピング公示システム(1000)が、この問合せに対してあて先通信ノード(4100)の動的な住所を応答する名前解決を行い、

(3) 発信元通信ノード(2000 又は 5300)が、前記応答されたあて先通信ノード(4100)を示す動的な住所あてに単に応答することを要求するサインを送り、

(4) あて先通信ノード(4100)が、答えるべき返事を新規のキャリア信号に載せて応答するカウンターサインを送ること。

3. (補正後) 請求項1の通信モデルにおいて、

発信元通信ノード(2000 又は 5300)に前記ホスト到達性を確認させる情報であって、あて先通信ノード(4100)から送られるものを発信元通信ノード(2000 又は 5300)に搬送する信号が用いられていることを特徴とする通信モデル。

4. (補正後) 請求項3に記載の通信モデルにおいて、

発信元通信ノード(2000 又は 5300)に前記ホスト到達性を確認させる情報が、あて先通信ノード(4100)が答えるべき返事である情報であり、該情報を搬送する信号が用いられていることを特徴とする

る通信モデル。

5. (補正後) 請求項3に記載の通信モデルにおいて、

あて先通信ノード(4100)が発信元通信ノード(2000 亦は 5300)に到達性を確認させる情報が、あて先通信ノード(4100)が答えるべき返事である情報とそれに加えられた附加情報であり、該情報を搬送する信号が用いられていることを特徴とする通信モデル。

6. (補正後) 発信元通信ノード(2000 亦は 5300)とあて先通信ノード(4100)とマッピング公示システム(1000)からなる、静的な識別子と動的な住所が関連付けられることによってホスト到達性が得られる蓄積交換網において、発信元通信ノード(2000 亦は 5300)とあて先通信ノード(4100)との間で情報をキャリアーする機能を有するキャリア信号であって、発信元通信ノード(2000 亦は 5300)からの応答要求に応じてあて先通信ノード(4100)が応答する場合において、答えるべき返事をキャリアーするキャリア信号。

7. (補正後) 請求項6に記載のキャリア信号において、答えるべき返事に加えてさらに附加情報をキャリアーすることを特徴とするキャリア信号。

8. (補正後) 発信元通信ノード(2000 亦は 5300)とあて先通信ノード(4100)とマッピング公示システム(1000)からなる、静的な識別子と動的な住所が関連付けられることによってホスト到達性が得られる蓄積交換網において、あて先通信ノード(4100)への到達性を発信元通信ノード(2000 亦は 5300)に確認させる到達性確認の方法であって、

発信元通信ノード(2000 亦は 5300)にあて先通信ノード(4100)への到達性を確認させる情報として任意の情報をマッピング公示システム(1000)に記憶させ、

発信元通信ノード(2000 亦は 5300)とあて先通信ノード(4100)とが所定の通信をすることによって、あて先通信ノード(4100)が発信元通信ノード(2000 亦は 5300)に対してした返信を前記記憶した任意の情報と比較することによって、あて先通信ノード(4100)への到達性の真偽を判定することを特徴とする到達性確認の方法。

9. (補正後) 請求項8に記載された到達性確認の方法において、

前記任意の情報が、あて先通信ノード(4100)における静的な識別子であることを特徴とする到達

性確認の方法。

10. (補正後) 請求項8に記載された到達性確認の方法において、

前記任意の情報が、あて先通信ノード(4100)として自己を発見させる際、発信元通信ノード(2000亦は5300)が問い合わせる静的な識別子に置き換えられたあらゆる文字列であることを特徴とする到達性確認の方法。

11. (補正後) 請求項8に記載された到達性確認の方法において、

前記任意の情報が、あて先通信ノード(4100)として自己を発見させる際、発信元通信ノード(2000亦は5300)が問い合わせる静的な識別子を變形することによって使用される變形ルールであることを特徴とする到達性確認の方法。

12. (補正後) 請求項8に記載の到達性確認の方法において、

あて先通信ノード(4100)の記憶装置に任意の情報を答えるべき返事として保存し、
あらかじめ合意された方式での通信に対して前記保存された情報を前記記憶装置より読み出し、
少なくとも該情報を含めたカウンターサインを返信することによって、あて先通信ノード(4100)が真のあて先通信ノード(4100)であることを発信元通信ノード(2000亦は5300)に確認させることを特徴とする到達性確認の方法。

13. (補正後) 請求項8に記載の到達性確認の方法において、

あて先通信ノード(4100)の静的な識別子を管理する複数のマッピング公示システム(1000)の内の1のマッピング公示システム(1000)を選択して正引き名前問合せをし、
参照するあて先通信ノード(4100)毎に異なるマッピング公示システム(1000)に切り替えることによって、あて先通信ノード(4100)の動的な住所を取得し、
前記取得した動的な住所を用いてあて先通信ノード(4100)と前記所定の通信をおこなうことを特徴とする到達性確認の方法。

14. (補正後) 請求項8から請求項13のいずれか一つに記載の到達性確認の方法において、

あて先通信ノード(4100)への到達性を確認することに失敗した場合に、所定の時間間隔を経過した後、再度請求項8から請求項13のいずれか一つに記載の到達性確認の方法を実施することによ

って、あて先通信ノード(4100)に対する到達性の真偽を確認することを特徴とする到達性確認の方法。

15.(補正後) 請求項8から請求項14のいずれか一つに記載の到達性確認の方法において、到達性を確認する機能を有しない端末に替わって、発信元通信ノード(2000 又は 5300)が到達性確認の方法を実施することを特徴とする到達性確認の方法。

16.(補正後) 請求項8 から請求項1 4 のいずれか一つに記載の到達性確認の方法において、前記到達性確認の結果を、所定の対象者及び公衆のうちの少なくとも何れか一方に通知することをさらに具備することを特徴とする到達性確認の方法。

17.(補正後) 請求項8 から請求項1 6 のいずれか一つに記載の到達性確認の方法において、発信元通信ノード(2000 又は 5300) が到達性確認する機能を有しない端末からのあて先通信ノード(4100)に対する到達性確認要求を受け、
発信元通信ノード(2000 又は 5300) があて先通信ノード(4100) に対する到達性の真偽を確認し、その結果を到達性確認する機能を有しない 端末に応答することを特徴とする到達性確認の方法。

18.(補正後) 請求項17に記載の到達性確認の方法において、到達性確認の結果を到達性確認する機能を有しない端末に 応答する際に、到達性確認する機能を有しない 端末がキャッシュの影響を受ける時間を予測して正常にアクセスできる時間をさらに前記 応答に含めることを特徴とする到達性確認の方法。

19.(補正後) 請求項8 から請求項1 4 のいずれか一つに記載の到達性確認の方法において、SNMP を用いてするネットワーク 管理の方法に先だって、あて先通信ノード(4100) への到達性確認を実施し、
ここであて先通信ノード(4100) への到達性が確認された場合には、到達性が確認されたあて先通信ノード(4100)の動的な住所を、SNMP を用いてするネットワーク 管理の方法に引き渡すことによって、動的に住所が変化するあて先通信ノード(4100)を管理することを特徴とする到達性確認の方法。

20. (補正後) 請求項8 から請求項14 のいずれか一つに記載の到達性確認の方法において、

到達性確認することによって、あて先通信ノード(4100)が網上に存在しないことが検知された場合には、マッピング公示システム(1000)が公示するあて先通信ノード(4100)に関する静的な識別子と動的な住所の関連付けを公示しないようにマッピング公示システムを構成しなおすことを特徴とする到達性確認の方法。

21. (補正後) 請求項20に記載の到達性確認の方法において、

到達性確認することによって、あて先通信ノード(4100)が網上に存在しないことが検知された場合には、あて先通信ノード(4100)の属するドメイン名を管理するDNSサーバにおいて、あて先通信ノード(4100)に関するリソースレコードの消込みをすることを特徴とする到達性確認の方法。

22. (補正後) 請求項8 から請求項14 のいずれか一つに記載の到達性確認の方法において、

蓄積交換網に発信元通信ノード(2000亦は5300)を示す静的な識別子を通知することを特徴とする到達性確認の方法。

23. (補正後) 請求項22に記載の到達性確認の方法において、

閉じた接続をすることを特徴とする到達性確認の方法。

24. (補正後) 請求項8 から請求項14 のいずれか一つに記載の到達性確認の方法において、

あて先通信ノード(4100)に関する到達性の確認が取れた住所を発信元通信ノード(2000 亦は5300)が記憶することによって、マッピング公示システム(1000)に対する名前解決過程を省略し、このことによって、マッピング公示システム(1000)に対するトラフィックを減ずることを特徴とする到達性確認の方法。

25. (補正後) プログラム製品であって、請求項8 から請求項24 のいずれか一つに記載の到達性確認の方法における到達性確認の結果を入力として用いることを特徴とするプログラム製品。

26. (補正後) プログラム製品であって、請求項8 から請求項24 のいずれか一つに記載の到達性確認の方法を計算機及びネットワーク接続機器の何れか一方に実行させることを特徴とするプログラム製品。

27. (補正後) コンピュータにより判読可能な媒体であって、請求項24から請求項25のいずれか一つに記載されたプログラム製品を格納したことを特徴とする媒体。

28. (補正後) 計算機及びネットワーク接続機器のうちの何れか一方である通信ノードであって、
 あて先通信ノード(4100)毎に少なくともサインが設定され、答えられるべき返事が前記あて先通信ノード(4100)を示す静的な識別子そのものでない場合には答えられるべき返事も設定され、前記あて先通信ノード(4100)に前記サインを送信する手段と、
 前記あて先通信ノード(4100)から応答されるカウンターサインを受信する手段と、
 前記受信されたカウンターサインによって搬送された答えるべき返事と前記設定された答えられるべき返事とを比較する手段を備え、
 比較された結果の真偽によってあて先通信ノード(4100)に対する到達性の真偽を確認することを特徴とする通信ノード。

29. (補正後) 請求項28に記載の通信ノードにおいて、
 あて先通信ノード(4100)の使用する静的な識別子を管理する複数のマッピング公示システム(1000)の内の1のマッピング公示システム(1000)を、前記あて先通信ノード(4100)毎に選択して正引き名前問合せをし、前記あて先通信ノード(4100)の動的な住所を取得して、あて先通信ノード(4100)と通信するために前記取得した動的な住所を用いておこなうことを特徴とする通信ノード。

30. (補正後) 請求項28から請求項29のいずれか一つに記載の通信ノードにおいて、
 あて先通信ノード(4100)への到達性確認に失敗した場合に、所定の時間間隔を経過した後、再度到達性確認を実施することによって、正しい到達性のあて先通信ノード(4100)に到達したか否かを確認することを特徴とする通信ノード。

31. (補正後) 請求項28から請求項30のいずれか一つに記載の通信ノードにおいて、
 一般利用者の使用する通信ノードからの要求に応じて、前記到達性確認をすることを特徴とする通信ノード。

32. (補正後) 請求項28から請求項31のいずれか一つに記載の通信ノードにおいて、

所定の対象者及び公衆のうち少なくとも何れか一方に、前記到達性確認の結果を通知することを特徴とする通信ノード。

33. (補正後) 請求項28から請求項32のいずれか一つに記載の通信ノードにおいて、

到達性確認する機能を有しない端末からのあて先通信ノード(4100)に対する到達性確認要求を受け、あて先通信ノード(4100)に対する到達性の真偽を確認し、その結果を到達性確認する機能を有しない端末に応答することを特徴とする通信ノード。

34. (補正後) 請求項33に記載の通信ノードにおいて、

到達性確認の結果を到達性確認する機能を有しない端末に応答する際に、到達性確認する機能を有しない端末がキャッシュの影響を受ける時間を予測して正常にアクセスできる時間をさらに前記応答に含めることを特徴とする通信ノード。

35. (補正後) 請求項28から請求項32のいずれか一つに記載の通信ノードにおいて、

到達性確認に後続する、SNMPを用いてするネットワーク管理の方法に接続するために、到達性が確認されたあて先通信ノード(4100)の動的な住所を、SNMPを用いてするネットワーク管理の方法に引き渡すことによって、動的に住所が変化するあて先通信ノード(4100)を管理することを特徴とする通信ノード。

36. (補正後) マッピング公示システム(1000)である通信ノードにおいて、

到達性確認することによって、あて先通信ノード(4100)の網上における不存在を検知したときに、マッピング公示システム(1000)におけるあて先通信ノード(4100)を示す静的な識別子と動的な住所からなる組の写像の公示を公示しないように変更することを特徴とする通信ノード。

37. (補正後) 請求項36に記載のマッピング公示システム(1000)である通信ノードにおいて、

到達性確認することによって、あて先通信ノード(4100)が網上に存在しないことが検知された場合に、あて先通信ノード(4100)の属するドメイン名を管理するDNSサーバにおいて、あて先通信ノード(4100)に関するリソースレコードの消込みをすることを特徴とする通信ノード。

38. (補正後) 請求項28から請求項30のいずれか一つに記載の通信ノードにおいて、

カウンターサインによってキャリーされた、蓄積交換網における発信元通信ノード（2000 亦は 5300）を示す静的な識別子の通知を受信する通信ノード。

39.（補正後）請求項38に記載の通信ノードにおいて、

事前に設定された蓄積交換網に発信元通信ノード(2000 亦は 5300)を示す静的な識別子を通知する通信ノードのみに対して、所定のサービスを提供する通信ノード。

40.（補正後）請求項28から請求項30のいずれか一つに記載の通信ノードにおいて、

あて先通信ノード(4100)に関する到達性の確認が取れた住所を記憶することによって、マッピング公示システム(1000)に対する名前解決過程を省略した通信ノード。

41.（補正後）請求項28から請求項40のいずれか一つに記載の通信ノードにおいて、

通信ノードの機能が、複数の装置によって共有されることを特徴とする通信ノード。

42.（補正後）プログラム製品であって、請求項28から請求項40のいずれか一つに記載の通信ノードにおいて計算機及びネットワーク接続機器の何れか一方に実行させるプログラム製品。

43.（補正後）コンピュータにより判読可能な媒体であって、請求項41から請求項42のいずれか一つに記載されたプログラム製品を格納したことを特徴とする媒体。

44.（補正後）発信元通信ノード（2000 亦は 5300）とあて先通信ノード（4100）とマッピング公示システム(1000)からなる、静的な識別子と動的な住所が関連付けられることによってホスト到達性が得られる蓄積交換網における、計算機及びネットワーク接続機器のうちの何れか一方であるあて先通信ノード(4100)であって、

住所の割当てを動的に受けてなる通信ノード及び外部ネットワークからは該通信ノードと一体となって参照される通信ノードのいずれかであり、

該通信ノードの記憶装置に、発信元通信ノード(2000 亦は 5300)がマッピング公示システム(1000)に前記あて先通信ノード(4100)を問い合わせる際に用いる任意の情報を答えるべき返事として保存し、サイン亦はあらかじめ合意された方式での通信の何れかに対して前記保存された情報を該記憶装置より読み出し、少なくとも該情報を含めたカウンターサイン亦はあらかじめ合意された方式での

通信に対する応答のうちの何れかを返信するように構成されることを特徴とする通信ノード。

45. (補正後) 請求項44に記載の通信ノードにおいて、

保存された答えるべき返事を、あて先通信ノード(4100)として発見させるために用いる静的な識別子であることを特徴とする通信ノード。

46. (補正後) 請求項44に記載の通信ノードにおいて、

保存された答えるべき返事を、発信元通信ノード(2000 亦は 5300)がマッピング公示システム(1000)に前記あて先通信ノード(4100)を問い合わせる際に用いる静的な識別子を置換した、あらゆる文字列で以って設定されるものであって、該文字列が該通信ノードの記憶装置に保存され、所定のポートへの通信要求を受けた際に、前記保存された文字列を該記憶装置より読み出し、少なくとも該文字列を含めた返信をするように構成されることを特徴とする通信ノード。

47. (補正後) 請求項44に記載の通信ノードにおいて、

保存された答えるべき返事を読み出した後、変形ルールに基づいて変形した文字列を少なくとも含めた文字列を返信するように構成されることを特徴とする通信ノード。

48. (補正後) 請求項45に記載の通信ノードにおいて、

ダイナミックDNSによって動的更新されるセンタ側マッピング公示システム(1000)において設定されるホスト名をFQDNでもって、該通信ノードに読み出し可能な文字列として設定されるものであって、該文字列が該通信ノードの記憶装置に保存され、所定のポートへの通信要求を受けた際に、前記保存された文字列を該記憶装置より読み出し、少なくとも該文字列を含めた文字列を返信するように構成されることを特徴とする通信ノード。

49. (補正後) 請求項44から請求項48のいずれか一つに記載の通信ノードにおいて、

待受けされる所定のポート以外に、少なくとも該通信ノードの設定変更用のポート及び一般の閲覧に供するためのウェブサービスを提供するウェルノウンなポートのいずれか一方のポートで待受けされるポートを備えるように構成されることを特徴とする通信ノード。

50. (補正後) 請求項42から請求項49のいずれか一つに記載の通信ノードにおいて、

答えるべき返事をキャリアするキャリア信号を、サインに回答して送出することによって発信元通信ノード(2000 亦は 5300)に自ノードへの到達性を確認させることを特徴とするあて先通信ノード。

51.(補正後) プログラム製品であって、請求項44から請求項50のいずれか一つに記載の通信ノードとしての機能を、計算機及びネットワーク接続機器の何れか一方に実現させるプログラム製品。

52.(追加) コンピュータにより判読可能な媒体であって、請求項54に記載されたプログラム製品を格納したことを特徴とする媒体。